

IN THE SPECIFICATION:

On page 1, replace the paragraph beginning on line one, with the paragraph shown below:

RELATED APPLICATIONS

This application is a non-provisional application claiming priority to U.S. provisional patent application serial number 60/105,891 filed on October 26, 1998, which is herein incorporated by reference, and is related to co-pending applications titled "Loading And Identifying A Digital Rights Management Operating System," U.S. patent application serial number 09/227611, "Key-based Secure Storage," U.S. patent application serial number 09/227568, "Digital Rights Management," U.S. patent application serial number 09/227559, and "Digital Rights Management Operating System," U.S. patent application serial number 09/227561, all filed on January 8, 1999 and assigned to the same assignee as the present application.

On page 1, delete the paragraph beginning on line 15 with the words "RELATED APPLICATIONS" and ending on line 24 with the words "present application."

On page 48, amend the paragraph starting on line 2 and ending on line 20 as shown below:

A general-purpose ~~central processing unit~~ processor (CPU) is configured with a new mechanism ~~that facilitates~~ facilitating an authenticated boot sequence. ~~The boot sequence that~~ provides the building blocks for client-side rights management when the system is online, and provides ~~for~~ continued protection of persistent data even when the system goes offline or is rebooted. The CPU is ~~manufactured with~~ includes a cryptographic key pair, and a manufacturer certificate testifying that the ~~manufacture~~ manufacturer built the CPU according to a known specification, ~~and an optional immutable symmetric key KS~~. The operating system (OS) includes a unique block of code, ~~referred to as the~~ or “boot block”. ~~An OS identity can be established from the boot block that can establish OS identity by extracting the identity~~ extraction from a digitally signed the boot block or by computing a hash digest of the boot block. During booting, the CPU executes a single opcode, followed by the boot block, as an atomic operation to set the identity of the ~~operating system~~ OS into the software identity register. ~~Execution of the opcode and the boot block is atomic, such that the software identity register is set to either the OS identity (i.e., boot block digest or OS public key) if the combined operation is successful, or zero if something subverts operation. Assuming success, the CPU appends the OS identity to its boot log. Following this authenticated boot sequence, the~~ The subscriber unit then can establish a chain of trust to prove its hardware and software to a content provider. ~~The subscriber unit stores content from the content provider in encrypted form using a storage key that is generated as~~

a function of OS specific and CPU specific data, so that it can be decrypted only on the same processor and by the specified OS.